

ADAM JOHN MACKINTOSH (*Pro Se*)
legal@ihughealth.com
P.O. Box 3364
Rancho Cordova, California 95741-3364
Telephone: (415) 767-0097
Facsimile: (415) 639-3388

FILED
DEC 24 2020
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTH DISTRICT OF CALIFORNIA

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

TSH

ADAM JOHN MACKINTOSH,

Plaintiff,

v.

APPLE, INC.;
UBER TECHNOLOGIES, INC.;
UBER HEALTH, LLC.;
JOSEF ACEBEDO; JERRY WANG; and
DOES 1-50

Defendants.

Case Name: Mackintosh v. Apple et. al.

Case No. **CV 20 9334**

COMPLAINT

JURY TRIAL DEMANDED

MACKINTOSH V. APPLE ET. AL.

1 Plaintiff, Adam John Mackintosh, by and through his inventions, right, title and interest
2 in patent applications, patent drafts (whether patentable or not), trademarks, intellectual property,
3 sketches, schematics, code, databases, healthcare business plans, product prototypes, photos,
4 videos, audio files and other competitive data (“iHug Trade Secrets”) alleges as follows:

5 INTRODUCTION

6 1. As alleged by Edward Snowden, a former United States National Security Agency
7 Officer; Richard Jacobs, a former United States Intelligence Agency Officer and Uber Security
8 Contractor; and Mat Henley, Nicholas Gicinto, Edward Russo, and Jacob Nocon Uber’s former
9 Security Team; Adam John Mackintosh (“Mackintosh”) further alleges Apple products, including
10 iPhone, among other computing devices (“Target Device”) can surreptitiously be accessed without
11 authorization or warning, and without a user’s knowledge.

12 2. In the years leading up to 2020, Uber Technologies Inc. (“Uber”), Apple Inc.
13 (“Apple”) and DOES influenced Jerry Wang (“Wang”), Josef Acebedo (“Josef”) and other
14 associated DOES to access and collect gigabytes of data containing trade secrets on early-stage
15 startups, and loaded the trade secrets onto Target Devices. Once the trade secrets were loaded on
16 Target Devices, Uber, Apple and DOES accessed these trade secrets through an organized and
17 repeating pattern of unauthorized activity within Target Devices. Through these collection
18 methods, Apple, Uber, and DOES believed they would surreptitiously capture American innovation
19 while it was in its infancy.

20 3. Mackintosh strongly believes in the benefits of fair competition, particularly in a
21 nascent field such as artificial intelligence in healthcare. Artificial Intelligence has the potential to
22 transform healthcare globally and become an essential industry. Artificial Intelligence will
23 eventually help us live healthier, live longer, and happier, a core value Mackintosh instilled at his
24 startup, iHug. Fair competition spurs new technical innovation, but what has happened here is not
25 fair competition. Instead, Apple, Uber and DOES have taken Mackintosh’s Artificial Intelligence
26 Operating System (“AiOS”) and iHug Trade Secrets in order to avoid incurring the risk, time, and
27 expense of independently developing their own technology that could spur their own innovation.
28

MACKINTOSH V. APPLE ET. AL.

1 4. Mackintosh developed a proprietary and confidential combination of novel methods
2 and processes, and formulas within his AiOS to handle and provide critical healthcare information
3 to manage our healthcare. Mackintosh experimented with, and ultimately developed a number of
4 different formulas that were aimed at cost-efficiencies in healthcare and rapidly prototyped various
5 wearable and stationary healthcare products that would operate within his AiOS. These trade secrets
6 will combine and optimize 37 core processes and methods over time which address various areas
7 in healthcare. Mackintosh's AiOS formed novel processes and methods that were non-existent in
8 healthcare, especially in the taxi, rideshare and wearable industry.

9 5. One example of a trade secret within AiOS is a proprietary sheet. The proprietary
10 sheet is unique in that Mackintosh spent significant time formulating this trade secret after reading
11 multiple healthcare books during his research and development, not limited to a Guide to the Laws
12 Governing the Practice of Medicine by Physicians and Surgeons. Mackintosh also studied courses
13 at Stanford Medical School relating to medical data sets and statistical healthcare data. The trade
14 secret contains four levels of grouped data sets that Mackintosh paired with two primary levels of
15 secondary variable data sets that combined unique operations, services, authority measures and
16 ranking based on compliance within federal healthcare laws. When combined with Mackintosh's
17 second proprietary algorithm as described below, it forms a core process within the AiOS.

18 6. Mackintosh's second proprietary algorithm creates the novel trade secret that allows
19 the consolidation and simplification of various areas in healthcare. These areas are complex and
20 balkanized, that create barriers to care. When these two trade secrets are intermittently and
21 concurrently executed, it creates interconnection and operability through a user interface on a
22 Target Device in healthcare amongst patients and healthcare providers. This trade secret allows
23 more open access to healthcare in an affordable and cost-effective platform.

24 7. The facts outlined above and elaborated further in this Complaint show that the
25 technology being developed, and currently being used within Uber, Apple and DOES healthcare
26 divisions, are from their theft and extrapolation of technology from Mackintosh's AiOS, iHug Trade
27 Secrets, codebase and is actually Mackintosh's healthcare technology.

28

1 8. Apple, Uber and DOES conduct alleged above and throughout this Complaint, has
2 given rise to this action for their unlawful racketeering and influence activity, including trade secret
3 theft, economic espionage, criminal infringement of copyrights, unauthorized computer access, and
4 unfair competition relating to Mackintosh's AiOS patent draft, and a substantial amount of other
5 novel healthcare material.

6 9. Ultimately, this surreptitious theft reportedly netted Uber and Apple billions of
7 dollars, allowed Uber to revive a stalled program, allowed Apple to transform its capabilities in the
8 Apple Watch and created novel Apple Health apps all at Mackintosh's expense.

9 10. In light of Apple, Uber and DOES misappropriation and infringement
10 of Mackintosh's AiOS patent drafts, iHug Trade Secrets and other novel technology,
11 Mackintosh brings this action before this Honorable Court to prevent any further misuse of
12 iHug Trade Secrets and to prevent Apple, Uber and DOES from harming Mackintosh's trade secrets
13 and the reputation of these trade secrets by misusing the technology, to protect the public's
14 confidence in the safety and reliability of Mackintosh's AiOS that he has long-sought to nurture,
15 and to obtain compensation for his damages, and for Apple, Uber and DOES unjust enrichment
16 resulting from their unlawful conduct.

17 PARTIES

18 11. Corporate Defendant, Apple, Inc. is a California corporation with its principal place
19 of business in Cupertino, California at the address of 1 Infinite Loop. Apple is the largest public
20 company in the world, with a current market capitalization of close to \$2 trillion.
21 Apple designs, markets and sells smartphones (including the iPhone), personal computers
22 (including Macs and Macbooks), tablets (including the iPad and iPod), wearables and accessories
23 (including the Apple Watch), and sells a variety of related products and services. Apple also owns
24 and operates the Apple App Store (the "App Store"), including contracting with Uber and other app
25 developers that distribute their applications ("apps") through the App Store and is therefore a party
26 to the anti-competitive, unlawful and unauthorized computer access, and the unconstitutional acts
27 at issues in this Complaint.
28

MACKINTOSH V. APPLE ET. AL.

1 12. Corporate Defendants, Uber Technologies, Inc. and Uber Health, LLC
2 (collectively “Uber”) are corporations formed under the laws of the state of Delaware with a place
3 of business at 1455 Market Street, San Francisco, California.

4 13. Individual Plaintiff, by and through his birth name, court-ordered married name and
5 any alias business names, Adam John Mackintosh is one in the same individual, who’s the Inventor
6 of the iHug Trade Secrets, Founder and Chief Executive Officer of iHug. Mackintosh is also
7 a Whistleblower and Witness to Apple’s native access methods into Target Devices and
8 Uber’s Hell Programs, and resides in the State of California.

9 14. Individual Defendants, Josef Acebedo is iHug’s former Chief Operating Officer
10 (“COO”) who resides in the State of California; Jerry Wang is iHug’s former Chief Technology
11 Officer and Sr. Software Engineer, who also resides in the State of California; and Defendant DOES
12 1-50 are persons or entities whose true names and capacities are presently unknown to Plaintiff,
13 who therefore, sues them by such fictitious names.

14 15. Plaintiff further alleges that each of the fictitiously named DOE Defendants
15 perpetrated or are otherwise liable as associated co-conspirators, agents, principals, aiders and
16 abettors for some or all of the wrongful acts alleged herein.

17 16. Each of the DOE Defendants are responsible in some manner for the matters alleged
18 herein and are jointly and severally liable to Plaintiff. Plaintiff will seek leave of Court to amend
19 this Complaint to state the true name and capacities of such fictitiously named DOE Defendants
20 when ascertained.

21 17. At all times mentioned herein and at all times relevant to this action, each associated
22 named Defendant and each DOE Defendant was the principal, agent, employer, employee,
23 individual, alter-ego, co-conspirator or aider and abettor of each of the other Defendants and was
24 acting within the course and scope of such corporate enterprise with knowledge authority
25 ratification and consent of the other Defendants.

26 18. Each of the aforementioned named Defendants described above herein is jointly and
27 severally liable to Plaintiff, based on the wrongful conduct alleged in this Complaint.
28

MACKINTOSH V. APPLE ET. AL.

JURISDICTION AND VENUE

19. The Court has federal question jurisdiction over the federal causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1331. The Court also has supplemental jurisdiction over the state law causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1367 because these claims arise out of the same nucleus of operative facts as Plaintiff's federal claims.

20. In addition, the Court has jurisdiction over all the causes of action in this Complaint pursuant to 28 U.S.C. § 1332 because complete diversity between the Plaintiff, Mackintosh, and each of the named Defendants exists, and because the amount in controversy exceeds \$75,000.

21. The Court has subject matter jurisdiction over claims of trade secrets, and intellectual property theft, and other related violations pursuant to the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961 et. seq.

22. This Court has personal jurisdiction over Defendants as they engaged in Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961 et. seq. and directed their actions at California residents in the Northern District of California.

23. The claims in this Complaint arise from Defendant's actions, including their unauthorized access into Target Devices, several of which are located in California.

24. As set forth above, at least one Defendant resides in this judicial district, and all Defendants are residents of the State of California.

25. In addition, a substantial part of the factual events or omissions giving rise to the claims alleged in this Complaint occurred in this Judicial District. Venue therefore lies in the United States District Court for the Northern District of California pursuant to 28 U.S.C. §§ 1391(b)(1) and (2).

26. Uber and Apple directly or through intermediaries, makes, distributes, offers for sale or license, sells or licenses, and advertises its products and services in the United States, the State of California, and the Northern District of California.

27. This Court has personal jurisdiction over Uber and Apple. Uber and Apple have conducted and does conduct business within the State of California and within this judicial district.

MACKINTOSH V. APPLE ET. AL.

FACTUAL ALLEGATIONS

A. Apple Pioneers An OS For iPhone

28. Similar to laptop and desktop personal computers, iPhones, iPads and other mobile computing devices require an operating system or “mobile OS” that enables multipurpose computing functionality. A mobile OS just like the operating system of any computer, is a piece of software that provides basic functionality to users of smartphones, such as button controls, touch commands, motion commands, and the basic graphical user interface, which includes icons and other visual elements representing actions that the user can take. A mobile OS also facilitates the basic operations of a smartphone, such as GPS positioning, camera and video recording, speech recognition and other features. In addition, a mobile OS permits the installation and operation of applications (“apps”). Apps are also operating systems that are compatible with mobile OS.

B. Uber Pioneers On-Demand Taxi Transportation

29. By 2016, Uber was so dominant that “Uber” was not only a noun to identify on-demand taxi rides, but also a verb that means “book a taxi ride”. Uber continued establishing the state-of-the-art in the taxi industry, which was solely predicated on an on-demand, mobile-to-mobile Application Program Interface (“Rideshare API”). Uber was losing many millions of dollars on its much-lauded, on-demand consumer ridesharing app, and had no presence in the healthcare market, much less the non-emergency medical transportation (“NEMT”) market.

C. Mackintosh Pioneers AiOS For A New Digital Healthcare System

30. By 2016, Mackintosh launched the first United States technology firm (“iHug”) to recognize a way to capture the transformative and commercial value of a new offering of healthcare through his AiOS. It made healthcare-related services safer, more efficient, and widely available through new methods and processes in healthcare, using a number of various individuals trained in healthcare (“Healthcare API”). This new AiOS was founded by Mackintosh after he conceptualized, hand-sketched, architected, engineered proprietary formulas and algorithms, and began digitizing them using Apple tools i.e. iPhone, iMac, Macbook, and iPad. He had successfully created a mobile-to-mobile platform that joined an on-demand API and Healthcare API process.

**D. Apple And Uber Pioneer Surreptitious Hell Programs To Steal Mackintosh's
AiOS For A New Digital Healthcare System And iHug Trade Secrets**

31. On information and belief, in order to gain backdoor access to a Target Device, Uber and DOES initiate code through Amazon Web Services, Inc. ("Amazon"), among other cloud-based servers. The servers are comprised of distributed and non-attributable ¹ architecture, network proxy, signaling and relay servers (collectively, "malicious servers"). ²

32. The collection of computer infrastructure causes unauthorized computer access to a Target Device using a Distributed-Denial-of-Service-style ("DDOS") attack, causing the Target Device to slightly heat up from the flood of modular malware. Once a connection is made, Uber accesses the core registry of the Target Device, as confirmed by cyber security experts. ³ Uber then initiates public, private, and native Apple-approved software ("Apple-code") to surreptitiously access, view and control a user's Target Device. ⁴

33. As set forth herein, Apple granted Uber *de facto* access into Target Devices.

34. Through Apple-code, Apple and Uber created Greyball, that enables various modular programs ("Hell Programs"). Uber's former Chief Security Officer, admitted Greyball ⁵ was modular in nature, having been "used for many purposes". Hell Programs are dangerous and pernicious to competition as each mode inherently stifles innovation across America. ⁶

¹ See Ex. A. Jacobs Letter ["Destruction of Records Using Non-attributable Hardware"].

² See Ex. B. Case 3:19-cv-07123 Facebook v. NSO - "the business of spying on your iPhone".

³ Cyber Security Expert's Tweet, "Main Binary UberClient... this application utilizes the IOKit Private Framework to read multiple registry entries from the device". [This Tweet was deleted from Twitter.]

⁴ See Ex. C "More disturbingly, the ability to see and record the frame buffer gives an attacker an effective keylogger since the frame buffer has access to login credentials. It's not clear if such a capability might have been available to well-written software, but if it had been, then you had the beginnings of a Trojan for iOS—something Apple has repeatedly said is not possible". See Ex. D "God View... Stalked journalists, celebrities, and ex-girlfriends". See Ex. E Uber Case CGC-18-571617 Uber's "secret capabilities in Uber's smartphone applications, and offensive intrusions into the privacy of users". See Ex. F. "Whistleblower Edward Snowden... Apple devices... can be used to snoop on an individual remotely and secretly".

⁵ See Ex. G "Uber received a subpoena from a Northern California grand jury seeking documents concerning how the software tool functioned and where it was deployed", and See Ex. H.

⁶ See Ex. I Uber's SEC filing, an Independent Expert's report was conclusive in his findings, and made a final decision that Uber did in fact steal trade secrets from another startup, Waymo.

1 **E. Loading Hell Programs. . .**

2 35. *First*, upon information and belief, and on that basis, Mackintosh further alleges in
3 each proceeding paragraph that Apple decentralized Greyball and Hell Programs by providing
4 non-attributable Apple hardware (“v-machine”) to Uber, Josef, Wang and DOES. *Second*, each
5 v-machine is layered with VMWare—a non-attributable virtual-based machine that masks
6 hardware identifiers i.e. internet protocol addresses. *Third* the v-machine is layered with a Virtual
7 Private Network (“VPN”) to encrypt internet traffic flow on MiFi devices and public WiFi’s so that
8 internet traffic does not have an origination point and does not appear from Uber or Apple’s
9 network. In sum, v-machines allow full anonymity, concealing interactivity, while Uber and DOES
10 are simultaneously connected to Uber and Apple’s servers and a user’s Target Devices.

11 36. *Fourth*, Defendants then acquire various unique identifiers, not limited to serial
12 numbers, UDID’s, and UUID’s of Target Devices after users purchase a Target Device, download
13 Uber’s applications, or through illicit fingerprinting tools or other manual methods, *See* Ex. J.
14 Apple uses a serial number to identify and track every bit of information on a user’s Target Device.
15 *Fifth*, upon information and belief, it’s further alleged Defendants presumably enter user’s Target
16 Device identifiers into an Apple command line terminal window that’s connected to Uber’s
17 malicious servers, allowing unauthorized connections to a user’s Target Device.

18 37. *Sixth*, Uber and DOES then plug-in a local Target Device into the v-machine to sync
19 with a mirroring and recording simulator—whilst installing Apple-code into Xcode—an
20 Apple-based coding tool—unlocking backdoor access to Apple products and other Target Devices.
21 *Seventh*, Uber and DOES then read and write to a user’s Target Device’s framebuffer, a part of the
22 Target Device memory that contains pixels and display data, bypassing all encrypted Apple security
23 features. As set forth above, upon information and belief, Uber and DOES can observe and
24 record a user’s screen activity, while mirroring apps from a user’s Target Device Graphics
25 Processing Unit (“GPU”). Through the methods and processes alleged above, Uber and DOES can
26 interact with a user’s apps on a second and separate local Target Device without warning, without
27 authorization, and without the user’s knowledge, ultimately permitting user impersonation.

28

F. Apple, Uber And DOES Are Late To Enter The Wearable And Healthcare Markets And Laid The Foundation To Steal iHug Trade Secrets Rather Than Compete Fairly In Healthcare

38. One of the most important technologies ever developed by Apple was the mobile OS software platform. It was formulated by passionate Apple employees under the direction of Steve Jobs and was first released in 2007. It's comprised of various Apple-code, that's interdependent on Target Devices. The infusion of Apple-code into Target Devices inherently creates permanent interactivity through a tertiary user interface layer between a competitor's brain and limbic system and the Target Device. Upon a later investigation, on information and belief, Mackintosh alleges when Target Devices are exploited, a competitor and others around the competitor can be exploited through use of Hell Programs as alleged in each proceeding section:

I. HELL PROGRAM – SCREEN RECORD

39. Apple's special permissions allowed Uber to use private Apple-code that allowed Uber to initialize various known and unknown Hell Programs, and various modes within Hell Programs, not limited to Hell Program "Screen Record". Screen Record mode allows Apple, Uber, and DOES to mirror and record a competitor's screen activity in real-time from the competitor's Target Device, not limited to apps and personal data.

II. HELL PROGRAM – DRAGNET

40. Apple, Uber and DOES also used Hell Program, "Dragnet". Dragnet mode is undocumented, unprecedented and extremely dangerous to competition. Mackintosh alleges while Josef, Wang and DOES Target Devices were in close proximity to Mackintosh's Target Devices, Dragnet mode surreptitiously accessed and instantaneously transferred system files from Mackintosh's Target Devices onto Josef, Wang and DOES Target Devices without warning or authorization, and without Mackintosh's knowledge. Upon information and belief, when Dragnet mode is active, system files are instantly compressed down from gigabytes to kilobytes during transmission. On information and belief, Apple, Uber and DOES initiated Dragnet mode to instantaneously extract hundreds of system files in seconds from Mackintosh's Target Devices.

III. HELL PROGRAM – SURVEILLANCE

41. Uber and DOES also remotely initiated “Surveillance” mode, to enable and disable the front and back facing camera and microphone on various Target Devices during private, personal and business interactions, including those pertaining to iHug Trade Secrets, allowing real-time video and audio feed from Mackintosh and other competitor’s Target Devices.

IV. HELL PROGRAM – IMPERSONATION

42. Impersonation mode has multiple capabilities, including the ability to mirror a competitor’s Target Device screen on a separate Target Device, allowing Apple, Uber and DOES to type, tap, and swipe through apps, essentially impersonating the competitor, while saving the screen recording through an auto-delete script leaving only a copy on the separate Target Device.

V. HELL PROGRAM – BOT

43. Bot mode is dangerous in that it uses a competitor’s internet reception to avert a trace, while sending multiple unauthorized requests for data collection also known as mobile scraping, and potential manipulation of code within the core registry a competitor’s Target Device, including prompting trade secrets to populate without human-intervention.

VI. HELL PROGRAM – SCREEN CAPTURE

44. Screen Capture mode is a sub-execution mode that’s initiated within Screen Record mode. Screen Capture mode allows Uber, Apple and DOES to remotely capture a competitor’s screen activity and/or facial expressions from the front-facing camera in real-time while Screen Record mode is active, much like a screen shot. Uber, Apple and DOES can surreptitiously screen capture their own activity while mirroring competitor’s Target Devices on a separate Target Device.

45. Each of the aforementioned known and unknown Hell Programs including Apple’s native access methods will collectively be referred herein as “Hell Programs”. Hell Programs are surreptitious in nature, and inherently accesses and caused to be accessed competitor’s Target Devices. Upon a later investigation, unbeknownst to Mackintosh at the time, and on information and belief, Mackintosh alleges in the years leading up to mid-2017 and thereafter, Apple, Uber and DOES initiated Hell Programs on Mackintosh’s Target Devices to

1 unlawfully collect data, and observed iHug Trade Secrets while Mackintosh was formulating them.
 2 During the investigation, on the information and belief, and on that basis, Mackintosh alleges, while
 3 Wang worked within Uber's Advance Technology Group, and Uber's Marketplace Analytics
 4 ("MA") Team as an off-the-books employee and/or third-party technology vendor, he
 5 communicated with Uber personnel, Uber's self-driving car unit and DOES. Uber used MA to
 6 target early-stage startups in competing business sectors to Apple, Uber and DOES to access and
 7 load trade secrets, codebase, and competitive intelligence, including deriving key business metrics
 8 of supply, demand, and functions of apps onto Target Devices.

9 46. Upon discovery of additional evidence Mackintosh recently uncovered, he further
 10 alleges Josef had special security clearances and after-hours access into Uber's Headquarters, and
 11 worked with Uber's Strategic Services Group ("SSG"). SSG collects data for Uber's in-house
 12 personnel or outside vendors, and supports the Intel, Investigations, and the MA teams.
 13 SSG frequently engages in fraud and theft, and employs third-party vendors to obtain unauthorized
 14 data. Upon information and belief, Josef transitioned to Uber's newly-formed Counter Intelligence
 15 Team during the Waymo-v-Uber trial. After the transition in March 2017, unbeknownst to
 16 Mackintosh at the time, Josef went on to illicitly support Wang on the ground at iHug's office.

17 47. By April 2017, Wang and Josef separately joined Mackintosh at iHug, and agreed
 18 to scale iHug into a nascent and embryonic market Mackintosh founded. On April 20, 2017, after
 19 Josef joined iHug, he eventually made his way into the position as iHug's COO.

20 48. On April 20, 2017, unbeknownst to Mackintosh, upon information and belief, Apple,
 21 Uber and DOES continued initiating Hell Programs to formulate new healthcare platforms and
 22 develop new healthcare products and services derived from iHug Trade Secrets, which subsequently
 23 created a new Delaware limited liability company, Uber Health, LLC.

24 49. Upon a recent discovery of evidence, on information and belief, by April 20, 2017,
 25 not only did Wang continue secretly downloading and compiling Mackintosh's competitive
 26 intelligence, codebase, and healthcare platform data totaling approximately 27,822 high-value files
 27 (**5.71 GBs**) of sensitive, secret, and valuable data—Josef assisted Wang in accessing physical iHug
 28

1 Trade Secret documents, and storage drives belonging to Mackintosh that contained iHug Trade
2 Secrets. These trade secrets were offline, never disclosed to anyone, safeguarded by Mackintosh
3 and with him at all times.

4 50. In particular, Mackintosh has uncovered evidence that Josef took extraordinary
5 efforts to access iHug Trade Secrets and conceal his activities. After Josef observed and learned
6 that Mackintosh kept his storage drives and trade secret documents with him at all times,
7 Josef staged a break-in at iHug's office. This prompted Mackintosh to purchase a digital access
8 PIN, stainless-steel locked safe ("safe") to protect the computer equipment in the office. Josef then
9 proceeded to ask for the digital pin to the safe to access and store the office computer equipment.
10 Naturally, Mackintosh began hiding his storage drives and physical trade secret documents inside
11 the safe believing they were inaccessible to any competitor and secretly secure.

12 51. Concurrently, Uber surreptitiously and routinely trained Uber employees and DOES
13 to implement and direct the almost-exclusive use of ephemeral and encrypted group communication
14 software ("chats"), including and not limited to Telegram, for the express purpose of destroying
15 illegal or unethical activity within their chats to avoid discovery in actual or potential litigation.

16 52. During the Waymo-v-Uber trial, after Uber was ordered to name the parties who
17 used the chats, Uber settled the case. Upon a later investigation, Uber, Wang, an Uber Manager and
18 DOES transitioned to a backup chat—a highly-sophisticated ephemeral and end-to-end encryption
19 chat that uses proprietary cryptography and pseudo-random encryption key generation algorithms
20 to encode plain text into ciphertext, making it indecipherable except the for intended person.

21 53. Upon a later investigation, on information and belief, at around the same time,
22 while Uber and DOES continued accessing Wang's compilation of iHug Trade Secrets from an app
23 on Wang's Target Device called Dropbox—a cloud-based file-storage system, the Uber Manager
24 was subsequently tasked with the development, iteration, and implementation of a significant
25 iHug Trade Secret that scaled globally and transformed Uber's operation. The transformation of
26 Uber's existing business divisions, and creation of entirely new business divisions at this point in
27 time is indicative to Uber's continued acquisition of iHug Trade Secrets.
28

1 **G. The United States Department Of Justice Opens An Investigation**

2 54. During the Waymo–v–Uber trial, the United States Department of Justice (“DOJ”)
3 opened a criminal investigation into Uber’s corporate structure and use of Greyball.

4 55. In light of the investigation, Defendants knowingly and willfully took a number of
5 steps with the intent to impede the investigation.

6 56. In one instance, Defendants and DOES repeatedly wiped their Target Devices upon
7 Uber and DOES acquisition of iHug Trade Secrets through use of Hell Programs.

8 57. In another instance, Josef, Wang and DOES began exploiting Target Devices and
9 other iHug servers as anonymous servers that are non-attributable to Uber, to covertly communicate
10 and compile iHug Trade Secrets, effectively aiding Uber in accessing the data without authorization
11 through Hell Programs. This organized and repeating pattern of activity averts forensic evidence of
12 transmission, communication and misappropriation of iHug Trade Secrets. By compiling iHug
13 Trade Secrets on non-attributable Target Devices and v-machines to Uber, Uber believed it would
14 avoid detection and never be subject to legal discovery. This is because a standard preservation of
15 evidence order typically focused on Uber work laptops, Uber networks, and Uber Target Devices.

16 58. In addition, unbeknownst to Mackintosh at the time, upon information and belief,
17 while Mackintosh progressively placed iHug Trade Secrets onto private and secure project boards
18 to assist Wang with building a healthcare platform, that’s an essential component to the
19 AiOS—Uber and DOES initiated Hell Programs on Josef, Wang and DOES Target Devices and
20 v-machines to extrapolate ideas from iHug Trade Secrets to build a new healthcare platform.

21 59. By summer 2017, Wang made his first in-person appearance at iHug’s office. Upon
22 a later investigation, unbeknownst to Mackintosh at the time, on information and belief, in a planned
23 intelligence collection operation, Josef supported Wang by granting him access to the safe at various
24 times throughout summer 2017 while Mackintosh was away from iHug’s office. Wang accessed
25 the safe and attached Mackintosh’s (**2 TBs**) storage drives to the USB ports on his v-machine. Wang
26 downloaded Mackintosh’s full codebase totaling approximately 101,485 files (**20.06 GBs**),
27 “Healthcare API” patent drafts, healthcare business plans and AiOS documents, a transformative
28

1 platform when combined. The patent drafts and codebase detailed technical information related to
2 an ever-changing model system with the potential to transform healthcare for millions of people
3 using automation through the AiOS. Upon information and belief, Wang confirmed his activity
4 through the chat. Uber, the Uber Manager and DOES later initialized Hell Programs on Wang's
5 Target Device and v-machine to extrapolate ideas from the data, while averting forensic evidence
6 of transmission, and misappropriation of iHug Trade Secrets, that reflected the results of
7 Mackintosh's years-long, intensive research into pain-points in healthcare.

8 60. Upon a later investigation, on information and belief, and on that basis,
9 Mackintosh alleges herein that Uber silently launched a new healthcare platform derived from iHug
10 Trade Secrets while Wang continued delaying the launch of Mackintosh's healthcare platform
11 during summer 2017. After the silent launch, Uber and DOES knowingly, willfully
12 and permanently deleted the Uber Manager's chat with Wang, and DOES to cover-up.
13 On August 25, 2017 at 12:01am, after the destruction of evidence, the Uber Manager
14 added a bitcoin address to receive 'illegal hush money payments,' a known corporate cover-up
15 practice at Uber, *See United States-v-Joseph Sullivan Case No. 320-71168-JCS.*
16 On August 25, 2017 at 7:20pm, after the corporate cover-up, prior to Wang's departure from iHug,
17 Wang attempted another systematic theft by surreptitiously setting up Agora within iHug's systems.
18 Agora is an artificial intelligence bot that collects ideas from cumulative conversations located in
19 multiple channels of communications. This would have allowed Uber and DOES to initiate Hell
20 Programs on Wang's Target Device to collect ideas as they were being formulated.

21 61. Upon a later investigation and evidence analysis, unbeknownst to Mackintosh at the
22 time, and on information and belief, around November 2017, while Mackintosh questioned Wang
23 about his delays and the state of the healthcare platform during a team meeting, Wang
24 surreptitiously initiated an unknown Hell Program on Mackintosh's Target Device to spoil
25 evidence. Upon a deeper analysis of evidence during the investigation, the front-facing camera
26 on Josef's Target Device inadvertently enabled while he was on the call. Wang recognized
27 Josef inside Uber's Headquarters, presumably heading into the infamous War Room,
28

1 and slyly initiated Hell Programs disabling the front-facing camera of Josef's Target Device, while
2 Uber and DOES eavesdropped from Uber's San Francisco Headquarters. At around the same time,
3 Uber integrated and launched yet another significant iHug Trade Secret into the Uber platform.

4 62. After Wang failed to timely deliver on multiple product deliveries, Josef terminated
5 Wang from iHug on November 7, 2017 at 2:13pm.

6 63. Upon a later investigation and discovery of evidence, on information and belief, after
7 Josef's departure from Uber's Headquarters, in anticipation of yet another planned intelligence
8 collection operation, on November 12, 2017 at 2:56pm, Josef secretly acquired a new v-machine.
9 In the months leading up to Josef's departure from iHug, he redirected and amassed approximately
10 26,317 iHug emails from various departments totaling (**1.17 GBs**) onto his Target Device and
11 v-machine, while he continued compiling other competitive intelligence. On information and belief,
12 Uber and DOES continued initiating Hell Programs on Josef's v-machine to extrapolate ideas.

13 64. During the recent investigation into Josef's activity, it was later discovered while
14 Mackintosh rapidly prototyped a new healthcare product to help hospitals and senior care facilities
15 for an upcoming partnership, Josef began compiling Mackintosh's research and development data
16 onto his new v-machine, including photographing the prototype on his Target Devices. Mackintosh
17 specifically designed the healthcare product for senior citizens, and vulnerable healthcare patients
18 who were being discharged from hospitals, and did not have a smartphone to book transportation
19 through an app. During the private healthcare product unveiling, high-value healthcare executives
20 asked Josef to do the honors of the unveiling. On information and belief, Uber and DOES remotely
21 initiated Hell Programs on a Target Device belonging to one of the healthcare executives, and
22 disabled his back-facing camera while he attempted to video record Josef out of excitement during
23 the unveiling. Months later, Uber launched a new product that reflected Mackintosh's healthcare
24 product and research and development data Josef compiled. Uber later boasted that it was the first
25 company in the world to develop this product in transportation.

26 65. Upon a later investigation and on information and belief, Uber continued initiating
27 Hell Programs on Josef and DOES Target Devices to extrapolate ideas from iHug Trade Secrets,
28

1 and on February 28, 2018 at 11:32pm, after Uber completed the development of a Healthcare API
 2 and launched the healthcare platform, Uber and DOES permanently deleted chats between Wang,
 3 the Uber Manager, it's Threat Operations division, and DOES, while Josef departed iHug.

4 66. After the destruction of evidence, on March 1, 2018, unbeknownst to Mackintosh at
 5 the time, upon information and belief, Uber launched a new Healthcare API, and announced
 6 features into its global operation that were derived from Mackintosh's "Healthcare API" patent
 7 draft and other iHug Trade Secrets that Uber and DOES ascertained through use of Hell Programs.

8 67. After Josef departed iHug around approximately March 2018, Wang and Josef
 9 joined a new Apple and Uber competitor in healthcare and NEMT, and devised a new fraudulent
 10 scheme to access and compile the startup's trade secrets onto Target Devices. Upon information
 11 and belief, and on that basis, Mackintosh alleges thereon that Josef formed a shell company, and
 12 misrepresented material facts during private meetings with the executives of the new startup. This
 13 prompted the disclosure of confidential pitch decks, healthcare business plans, operational data
 14 including and not limited to vehicle makes, models and expenditures, employee data including and
 15 not limited to salaries, commissions and other competitive healthcare and NEMT data. Wang, Josef
 16 and DOES presumably compiled the data onto Target Devices, v-machines, and within the emailing
 17 servers among other systems belonging to the new startup that are non-attributable and anonymous
 18 to Uber, and DOES, while Uber and DOES continued initiating Hell Programs on Wang, Josef and
 19 DOES Target Devices and v-machines to unlawfully access and acquire such valuable data.

20 **H. Mackintosh Verifies His Growing Suspicion That Uber and Apple Have Stolen**
 21 **iHug Trade Secrets and Confidential and Proprietary Intellectual Property**

22 68. During a later investigation, video evidence surfaced in late 2019 of Uber's
 23 healthcare platform in operation, that bears a striking resemblance to iHug Trade Secrets.

24 69. Mackintosh further discovered that, not only has Uber improperly executed on
 25 iHug Trade Secrets, Uber has created one, and potentially other situations, that caused the fatality
 26 of a senior citizen in healthcare from the improper execution of iHug Trade Secrets. In another
 27 instance, Mackintosh discovered yet another video of an Uber driver who was visually frustrated
 28

1 and threatened to choke off the oxygen tank of a senior citizen during a hospital discharge.

2 70. Mackintosh has recently discovered that an independent expert report has since been
3 deleted from Twitter. The report was produced by a Global Security Expert who's familiar with
4 OS for iPhone. This report is a key piece of evidence to this action. The report was conclusive in
5 its findings, relating to Apple allowing Uber authorized and/or unauthorized access into user's
6 Target Devices core registry. The report entailed key pieces of evidence that were generated using
7 a Professional Disassembler and Debugger ("IDA")—an IDA is an interactive, programmable,
8 extensible, multi-processor disassembler. This IDA system is a *de-facto* standard for the analysis
9 of hostile code, and used for vulnerability research on newly released products and services.

10 71. In another apparent corporate cover-up, a video of the IDA test that shows Uber's
11 applications accessing the core registry entries of a Target Device had been deleted from Twitter.

12 72. In yet another apparent corporate cover-up, Mackintosh discovered more deletions
13 pertaining to Hell Programs, specifically, a very particular read-out from Verify.ly—a platform and
14 systems scanner that processes and produces a human-readable report, detailing all detected,
15 common security issues within an OS and other smartphone operating systems. Further, within the
16 deleted Global Security Expert report details, several screen shots showed Apple's special
17 entitlement key was still in use within Uber's applications, and marked as "TRUE". Apple has
18 stated under oath to Congress, that it will not write software that allows backdoor access into Target
19 Devices. Upon information and belief, and on that basis, Mackintosh alleges Apple willfully
20 continued allowing Uber to use a key to the backdoor of Target Devices. Other substantive evidence
21 from the report had also been deleted from Twitter.

22 73. Mackintosh recently discovered more evidence that prior to the DOJ's investigation
23 into Uber leading up to May 5, 2017, Josef surreptitiously engaged in fraud and theft within weeks
24 of joining iHug. Specifically, while Mackintosh stepped away from his suitcase containing iHug
25 Trade Secrets, Josef presumably rummaged through the documents and took a photo of at least one
26 or more documents on his Target Device. Shortly after the DOJ's investigation commenced in
27 early-May, Josef claimed his Target Device "wiped by itself" on May 15, 2017 at 9:50pm.

28

I. Mackintosh has Been, And Will Be, Severely Harmed By Apple and Uber's Theft of iHug Trade Secrets And Misappropriation Of Mackintosh's Confidential And Proprietary Trade Secret Information

74. Mackintosh founded iHug after the pain and loss of his loved ones, and went to great expense and sacrifice, and years of painstaking development to invent the AiOS, healthcare API, healthcare platform, healthcare business plans and other confidential and proprietary information.

75. Uber and Apple have purposefully, actively, and voluntarily distributed an AiOS, healthcare platform, healthcare API, healthcare business plans and related products and services with the expectation that they will be purchased, used, or licensed by consumers in the Northern District of California and beyond. Defendant's actions, omissions, and public disclosure of iHug Trade Secrets to competitors and others, have destroyed the value of iHug Trade Secrets, interfered with and wholly injured Mackintosh's ability to compete using his iHug Trade Secrets.

76. Uber, Apple and DOES have thus committed acts of illegal acquisition and use of iHug Trade Secrets within the State of California and, particularly, within the Northern District of California. Uber and Apple's willful, malicious, and calculated exploitation of stolen iHug Trade Secrets greatly harmed Mackintosh's genuine efforts to form and grow an embryonic and nascent market that was intended to help our loved ones live healthier, live longer, and happier through iHug Trade Secrets. Uber's use of, and not limited to, a healthcare platform and healthcare API derived from iHug Trade Secrets, has been and continues to be purchased, used, and licensed by consumers during the COVID-19 Pandemic, and continues to profit from iHug Trade Secrets at Mackintosh's detriment. By purposefully distributing multiple services derived from iHug Trade Secrets, Uber and Apple have injured Mackintosh and is thus liable to Mackintosh for theft of and illegal use of the iHug Trade Secrets at issue pursuant to the proceeding causes of action.

77. With this Complaint, Mackintosh ("Plaintiff") seeks to vindicate his rights, prevent further infringement of his patent drafts, intellectual property, copyrighted work, and other iHug Trade Secrets, preclude any further misuse to prevent loss of life, obtain compensation for damages and for the Uber, Apple and DOES unjust enrichment resulting from their unlawful conduct.

FIRST CAUSE OF ACTION

Violation of Federal Defense of Trade Secrets Act 18

Against Uber and Apple

78. Plaintiff owns all right, title and interest in iHug Trade Secrets described herein.

79. Plaintiff owns and possesses certain confidential, proprietary, and trade secret information, as described above.

80. Plaintiff's trade secret information further includes a perpetual platform that runs an API that combines multiple healthcare and mass market sectors within the AiOS. This trade secret enjoins with the second proprietary algorithm and proprietary sheet, which open up access to healthcare to a user with a Target Device.

81. Another example of a trade secret within Plaintiff's AiOS was something he learned while working in the private sector under a California State Program. It was not a process or method within taxi or rideshare. It's also another core element within the AiOS that allows the second proprietary algorithm, proprietary sheet and perpetual platform to operate as described above. The core element contains multiple user traffic splits, with continuous pings, connections and validation controlled by server managers including authentication and redundancy protocols that enjoin with a fifth example of Plaintiff's AiOS trade secrets.

82. The fifth example was Plaintiff's understanding that the biggest pain point in healthcare is labor expense. Plaintiff formulated an artificial intelligence algorithm. These parts lower the operational costs on the healthcare system side, while efficiently offering variable data sets through an array that connect with the user. The trade secret within the AiOS automatically expands with the degree of evolution in healthcare, and formulates data sets with the trend of societal input, and over time, advances supply and demand, and the technological evolution in automation. The trade secret can process millions of transactional requests with minimal labor expense output. It consists of a main server and code within it, auto-population, input layers, hidden layers, data sets and process of information, among other methods and processes that create an artificial input / output source, including a timer that has variable time settings based on data sets.

MACKINTOSH V. APPLE ET. AL.

1 This trade secret lowers American's healthcare expenses, and cures roadblocks to accessibly, while
2 driving down healthcare operational costs.

3 83. Due to the potential commercial value of the iHug Trade Secrets, Plaintiff set in
4 place, reasonable, substantial and stringent preservation and safeguard measures.

5 84. For instance, iHug Trade Secrets were located on storage drives, were offline, were
6 locked in a safe and stored inside a cargo trailer that used bolt-cutter proof locks and one inch
7 stainless-steel plates on the door, including an alarm system with proximity sensors, while parts of
8 the technology were stored on highly-secured databases and other cloud-based servers and services
9 that Plaintiff set long-tail complex passwords.

10 85. Plaintiff also kept various and specific trade secrets memorized, and did not digitize
11 them until needed to complete other trade secrets. At various times, Plaintiff digitized the trade
12 secrets onto secure and private project boards, including action items and other technology-stacks
13 that Plaintiff provided to Wang.

14 86. Plaintiff not only kept various trade secrets memorized, he also kept various trade
15 secrets in form of sketches, schematics, flow charts, procedures, question and answers and printed
16 paper patent drafts that were located inside his secured cargo trailer.

17 87. Plaintiff also kept various trade secrets in audio format on his Target Device, as
18 reference points to remind him of healthcare trade secrets to digitize, democratize and globalize.

19 88. By way of further example of Plaintiff's efforts to keep parts of the AiOS secret, he
20 required every individual who entered iHug's office to sign NDA's barring them from disclosing
21 iHug Trade Secrets and other data. Individuals and entities were also frequently reminded of their
22 confidentiality obligations to Plaintiff.

23 89. Plaintiff has at all times maintained stringent security measures to preserve the
24 secrecy of the iHug Trade Secrets. For example, Plaintiff restricts access to confidential and
25 proprietary trade secret information to only those who "need to know". That is, employees,
26 contractors and/or partners among others, working on projects unrelated to the AiOS, healthcare
27 platform, and Healthcare API have not had and do not have access to Plaintiff's codebase,
28

1 schematics, or other categories of confidential and proprietary information.

2 90. All networks hosting Plaintiff's confidential and proprietary information have been
3 and continue to be secure and have at all times required long-tail passwords and two-factor
4 authentication. Target Devices that were provided to Plaintiff's employees, contractors and/or
5 partners are encrypted, password protected, and subject to other Apple security measures.

6 91. Plaintiff secured iHug's physical facilities at all times by limiting and restricting
7 access, assigning and keeping track of office keys, including routinely changing the safe digital pin
8 among other safeguards.

9 92. Due to these security measures, Plaintiff's confidential and proprietary trade secret
10 information is not available for others in the NEMT, ridesharing and the healthcare industry—or
11 any other industry—to use through any legitimate means.

12 93. The proprietary and technical information, i.e., iHug Trade Secrets that Apple, Uber
13 and DOES ("Corporate Defendants") obtained, constitutes trade secrets because Plaintiff, as
14 described herein, derived independent economic value from that information and keeping that
15 information secret; Such information is not generally known or readily ascertainable by proper
16 means from other persons who can obtain economic value from its disclosure or use; Because
17 Plaintiff has and continues to undertake efforts that are reasonable under the circumstances to
18 maintain the secrecy of the trade secrets described herein is not and was not generally known to
19 competitors. Plaintiff's confidential, proprietary, and trade secret information derives independent
20 economic value from not being generally known, and not being readily ascertainable through proper
21 means by another person who could obtain economic value from the disclosure or use of the
22 information.

23 94. Apple and Uber also ascertained iHug Trade Secrets at various times on Plaintiff's
24 Target Devices and through associated individuals Target Devices through use of Hell Programs,
25 and upon information and belief, from Apple's own App Store infrastructure that stores repositories
26 of App Developer's "competitor's" codebase.

27 95. The organized and repeating pattern of activity and influence alleged in this
28

1 Complaint, bypasses any and all stringent and reasonable measures Plaintiff took, or could have
2 taken to protect iHug Trade Secrets either physically or digitally.

3 96. The malicious and fraudulent acts and creation of Hell Programs that contain
4 computer containments not limited to malicious code and malware, and native access methods,
5 unlawfully bypassed Plaintiff's stringent and protective measures, and circumvented all
6 Apple-leading security features in its entirety.

7 97. At the time the Corporate Defendants acquired iHug Trade Secrets, the Corporate
8 Defendants knew they acquired such Trade Secrets through improper unauthorized computer
9 access.

10 98. Plaintiff further alleges the Corporate Defendants improperly obtained and used
11 such iHug Trade Secrets in part or in whole, and extrapolated trade secret information derived from
12 iHug Trade Secrets, in the planning of, design of, marketing of and sale of the Corporate Defendants
13 and all affiliated entities, i.e. Uber Health, Uber Works and Uber for Business and secret projects
14 at Apple after extrapolating iHug Trade Secret data and integrated it within Apple Watch and Apple
15 Health.

16 99. Plaintiff's confidential, proprietary, and trade secret information relates to products
17 and services used, sold, shipped and/or ordered in, or intended to be used, sold, shipped and/or
18 ordered in, interstate or foreign commerce.

19 100. Plaintiff's trade secret technical information, designs, healthcare business plans, and
20 other "know how" related to his AiOS, constitute trade secrets as defined by the Federal Defense
21 of Trade Secrets Act.

22 101. In violation of Plaintiff's rights, the Corporate Defendants misappropriated
23 Plaintiff's confidential, proprietary and trade secret information in an improper and unlawful
24 manner as alleged herein. The Corporate Defendants misappropriation of Plaintiff's confidential,
25 proprietary, and trade secret information was intentional, knowing, willful, malicious, fraudulent,
26 and oppressive. The Corporate Defendants have concealed, attempted and continue to attempt to
27 conceal their misappropriation.

28

1 102. Absent injunction, the Corporate Defendants will continue to misappropriate and
2 use iHug Trade Secrets for their own benefit and to Plaintiff's detriment. The Corporate Defendants
3 knew or should have known under the circumstances that the information misappropriated by the
4 Corporate Defendants were trade secrets.

5 103. Upon information and belief, and on that basis, Mackintosh alleges the Corporate
6 Defendants knew or should have known Plaintiff had no knowledge, or even the concept of
7 Hell Programs, and trusted Apple, and would never think Apple would gain native access into
8 Target Devices, as it's the equivalent to hacking and exploiting a competitor's brain, thoughts and
9 actions.

10 104. Plaintiff had no defense in preventing the Corporate Defendants and DOES
11 unauthorized access into his Target Devices to access without permission and misappropriated
12 iHug Trade Secrets and other personal and competitive data without authorization, without warning
13 and without Plaintiff's knowledge.

14 105. As the direct and proximate result of the Corporate Defendants conduct to use Josef,
15 Wang and DOES ("Individual Defendants") through brand power and influence to access and
16 compile iHug Trade Secrets onto Target Devices and v-machines, Plaintiff has suffered and, if
17 Defendant's conduct is not stopped, Plaintiff will continue to suffer severe competitive harm,
18 irreparable injury, and significant damages, in an amount to be proven at trial.

19 106. As an actual and proximate cause of the Corporate Defendants trade secret
20 misappropriation, Plaintiff suffered damages in the amount to be proven at the time of trial, but
21 which are in excess of the minimum jurisdiction of this Court.

22 107. Because Plaintiff's remedy at law is inadequate, Plaintiff seeks, in addition to
23 damages, temporary, preliminary, and permanent injunctive relief to recover and protect his
24 confidential, proprietary, and trade secret information and to protect other legitimate business
25 interests.

26 108. Plaintiff's business operates in a competitive market and will continue suffering
27 irreparable harm absent injunctive relief.
28

SECOND CAUSE OF ACTION

California Uniform Trade Secret Act Cal. Civ. Code §§ 3426 *et seq.*

Against All Defendants

109. Plaintiff incorporates all of the above paragraphs as though fully set forth herein.

110. Plaintiff's trade secret described in this Complaint constitute trade secrets as defined by California's Uniform Trade Secrets Act.

111. A sixth example as to Plaintiff's AiOS, Plaintiff invented another proprietary algorithm. When executed, several bi-directional input / output data sets continuously run, learn and process data. These processes and methods can detect, and suppress hereditary diseases and healthcare trends. The formula was invented by Plaintiff in an effort to suppress and/or slow the progression of hereditary diseases after the loss of his loved ones during his younger years and later in his adulthood. As stated above herein, Plaintiff's entire AiOS has the capability and scalability to grow with society and the demand of the ever-changing healthcare system, and our physiology, as the world is rapidly transitioning out of the industrial age, into the technological age and now the artificial intelligence and automation age. These algorithms, processes and methods described above and the trade secrets at issue did not exist in the taxi, healthcare or rideshare markets Plaintiff targeted, and have actual or potential independent economic value from not being generally known to the public or other persons who could obtain economic value from their disclosure or use.

112. As for a seventh example of a trade secret, as to Plaintiff's AiOS, the seventh trade secret is powered by the sixth trade secret and each preceding trade secret. It's a particular data flow method that organizes, learns, and perpetuates as data changes. This trade secret is significant and another core process and method within the AiOS. It consists of various functions and input into a Target Device or Wearable Device that stores the data, and uses various layers to display the data to the user. As the user interacts with and inputs the data, the specific trade secret will provide a response to the user outlining next steps, recommendations of various data sets and the arrays within those data sets. When this trade secret is used to opt-in or tap on, various data sets and arrays within those data sets create a prompt, the user is provided with option to use tangible assets or other

1 options. This trade secret is essential to the proprietary sheet and second proprietary algorithm as
2 described above. When all three trade secrets are combined, it creates a transformative operation
3 process that opens up access to healthcare on a variable mode as to the eighth trade secret. When
4 this trade secret is used with the various trade secrets described herein, it groups families, friends
5 and even their corporate employers to open up even more access to the user. Specifically, there
6 are variable data sets that can be updated over time, to include split, grouped or otherwise shared
7 data-set-links among users to open up more healthcare services to the user.

8 113. As a direct and proximate result of the Corporate Defendants and Individual
9 Defendants conduct, Plaintiff is threatened with injury and has been injured in an amount in excess
10 of the jurisdictional minimum of this Honorable Court and that will be proven at trial.

11 114. Plaintiff has also incurred, and will continue to incur, additional damages, costs and
12 expenses, including attorney's fees upon retention of counsel, as a result of the Individual
13 Defendants misrepresentation, omissions, and fraud, and Corporate Defendants misappropriation.

14 115. As a further proximate result of the misappropriation and use of Plaintiff's trade
15 secrets, the Corporate Defendants were unjustly enriched.

16 116. The Corporate Defendants and Individual Defendants conduct constitutes
17 transgressions of a continuing nature for which Plaintiff has no adequate remedy at law. Unless
18 and until enjoined and restrained by order of this Court, the Corporate Defendants will continue to
19 retain and use Plaintiff's trade secret information to enrich themselves and divert business from
20 Plaintiff.

21 117. Pursuant to California Civil Code § 3426.2, Plaintiff is entitled to an injunction
22 against the misappropriation and continued threatened misappropriation of trade secrets as alleged
23 herein and further asks the Court to restrain the Corporate Defendants from using all trade secret
24 information misappropriated from Plaintiff and to return all trade secret information to Plaintiff.

25 118. The acts and/or omissions of the Corporate Defendants and Individual Defendants
26 as described herein were willful and malicious within the meaning of California Civil Code section
27 3426.3(c) and requests exemplary damages that will be awarded at the time of trial.

28

THIRD CAUSE OF ACTION

Violation of Comprehensive Computer Data Access and Fraud Act

California Penal Code § 502

Against All Defendants

119. Plaintiff incorporates paragraphs 1 – 77 above as though fully set forth herein.

120. Through the acts and/or omissions as alleged above in paragraphs 1 – 77, the Corporate Defendants either individually or jointly committed violation of Cal. Penal Code § 502(c)(2), (3), (4) and (7) because they intentionally accessed, and initiated Apple's native access methods without authorization, and/or Hell Programs that caused to be accessed (a) Plaintiff's computers, and protected computers, and (b) the and Individual Defendants and DOES Target Devices and v-machines (c) while Corporate Defendants initiated Hell Programs to gain exploited unauthorized access into Target Devices and v-machines to obtain iHug Trade Secrets.

121. As alleged by Uber's former Security Team, Uber "unlawfully collected information from the mobile phones of Uber opponents", and that Uber has "secret capabilities in Uber's smartphone applications", and engages in "offensive intrusions into the privacy of users", which supports Plaintiff's allegations herein.

122. The acts and/or omissions of the Corporate Defendants and Individuals Defendants as described above were made with malice, fraud and/or oppression as those terms are used in California Civil Code section 3294. To the extent such acts and/or omissions were made by the Individual Defendants, such individuals were managing agents and/or Corporate Defendants ratified the wrongful conduct for which the damages are sought.

123. The Corporate Defendants violated Cal. Penal Code § 502 as they knowingly and with intent to defraud, accessed and caused to be accessed (a) Plaintiff's protected computers and other computing devices; (b) Target Devices (c) the Individual Defendants Target Devices and (d) the Individual Defendants v-machines without authorization, and by means of such conduct, furthered the intended fraud and obtained something of value.

124. The Corporate Defendants knowingly, willfully and with full intent accessed and

MACKINTOSH V. APPLE ET. AL.

1 without permission, altered and used iHug Trade Secrets, competitive data including physical trade
2 secret documents through a computer system, and computer network in order to (a) devise and
3 execute a scheme artifice to defraud and deceive, and (b) wrongfully control and obtain money,
4 property, and data in violation of California Penal Code § 502(c)(1).

5 125. The Corporate Defendants knowingly and without permission used and caused to
6 be used Plaintiff and Individual Defendants Target Devices, data processing devices, servers
7 and other computers located in California among other states, and in violation of California Penal
8 Code § 502(c)(3). For instance, upon information and belief, after the Corporate Defendants
9 initiated Hell Programs to unlawfully login to iHug's Google Business G-Suite systems, Google
10 sent an automated alert which stated, "A lesser secure app", attempted to login to your account.

11 126. In another instance as alleged above, after a later investigation, on information and
12 belief, upon the Corporate Defendants unauthorized and/or exploited access into the Individual
13 Defendants Target Devices, an IP address was recorded. The Individual Defendants sent an
14 unsolicited text to Plaintiff claiming someone had hacked the iHug email to cover-up.

15 127. Upon a later investigation, in yet another instance of unauthorized computer access,
16 upon information and belief, while Plaintiff was away from iHug's office, the Corporate Defendants
17 surreptitiously initiated Hell Programs on Plaintiff's iMac located in iHug's office, and unlawfully
18 accessed the iMac's framebuffer to click on folders, apps and other data. This effectively allowed
19 the Corporate Defendants access to iHug Trade Secrets and Plaintiff's personal identifiable
20 information located on the iMac without authorization.

21 128. The Corporate Defendants knowingly and without permission and/or authorization,
22 provided and assisted in providing means of accessing Plaintiff's Target Devices, computers,
23 computer systems, and computer networks through use of Hell Programs in violation of California
24 Penal Code § 502(c)(6).

25 129. The Corporate Defendants knowingly and without permission accessed and caused
26 to be accessed Plaintiff's computers, computer systems, and computer networks, including those
27 located in California, in violation of California Penal Code § 502(c)(7).

28

1 130. The Corporate Defendants knowingly injected computer contaminants into
2 Plaintiff's Target Devices and computers, to gain unauthorized access to computer networks in
3 violation of California Penal Code § 502(c)(8).

4 131. The Corporate Defendants knowingly used Apple-code and paired it with computer
5 contaminant and injected it into Target Devices and computer networks allowing the creation of
6 illegal software known to many as Greyball, and the Hell Programs within Greyball, and all inherent
7 modes embedded within it in violation of California Penal Code § 502(c)(8).

8 132. The Corporate Defendants and Individual Defendants willful, knowing, malicious
9 and unlawful actions, caused Plaintiff to incur losses and damages, including his time, and among
10 other things, the expenditure of resources to investigate and remediate Corporate Defendants and
11 Individual Defendants conduct and damage to Plaintiff, and damage to the relationships and
12 goodwill between Plaintiff and iHug users, and potential iHug users.

13 133. As a result of the fraud, the Corporate Defendants unlawfully gained a competitive
14 advantage, and obtained investments, money, customers, remote access and control of Target
15 Devices, and allegedly recruited corrupt attorneys to protect their corporate conduct using the
16 investment and monies gained from the fraud, the value of which exceeds \$5,000. Not only did the
17 Corporate Defendants use the investment and monies alleged above, the Corporate Defendants used
18 it to hire the world's top talent to build on the misappropriated trade secrets to fraudulently cover-
19 up and obfuscate the theft.

20 134. The Corporate Defendants and Individual Defendants each violated Cal. Penal Code
21 § 502 by conspiring to commit the violations alleged in the proceeding paragraphs.

22 135. Pursuant to Cal. Penal Code § 502(e)(1), Plaintiff is entitled to compensatory
23 damages and other equitable relief based on such violations including all expenditures reasonably
24 and necessarily incurred by Plaintiff to verify that Plaintiff's computer systems were not altered,
25 damaged or deleted by the access.

26 136. As alleged in paragraphs 1 – 77, and allowable under California Panel
27 Code §§ 502(e)(1), and (2), Plaintiff is entitled to injunctive relief.
28

FOURTH CAUSE OF ACTION

Violation of Computer Fraud and Abuse Act 18 U.S.C. § 1030

Against All Defendants

137. Plaintiff incorporates paragraphs 1 – 77 above as though fully set forth herein.

138. At all times relevant to this action, the Corporate Defendants accessed, used, or caused to be accessed or used, Plaintiff's and Individual Defendants Target Devices without authorization to improperly ascertain iHug Trade Secrets with the intent to use the iHug Trade Secrets.

139. Plaintiff's servers, data processing devices, and Target Devices are "computers" as defined by 18 U.S.C. § 1030(e)(1); and "protected computers" as defined by 18 U.S.C. § 1030(e)(2)(B) and being "used in or affecting interstate commerce or communication".

140. Corporate Defendants and Individual Defendants malicious servers, relay servers, signaling servers, proxy servers, Uber's apps, Apple's native access methods, App Store, various Hell Programs hosted on Amazon, Apple's servers and platforms, and other malicious servers, virtual private network services, ephemeral end-to-end encrypted messaging and file-sharing software, iMacs, iPhones, iPads, Macbooks and other computing machines, Apple-code not limited to special entitlements, private IOKits, private frameworks and other private and secret Apple OS platform code that's interdependent on the pre-installed OS on Target Devices are "computers" as defined by 18 U.S.C. § 1030(e)(1).

141. The Corporate Defendants violated 18 U.S.C. § 1030(e)(2) because they intentionally accessed and caused to be accessed (a) Plaintiff's and Individual Defendants computers, and (b) Target Devices, without authorization and, obtained data from the Target Devices.

142. The Corporate Defendants violated 18 U.S.C. § 1030(a)(4) as they intentionally defrauded and accessed and caused to be accessed (a) Plaintiff's and the Individual Defendants protected computers and (b) Target Devices without authorization, and by means of such conduct furthered the intended fraud and obtained something of value.

MACKINTOSH V. APPLE ET. AL.

1 143. The Corporate Defendants continued fraud also includes sending unauthorized
 2 commands to Plaintiff's and the Individual Defendants Target Devices, protected computers and
 3 computer networks, and concealed the commands through Hell Programs and malicious servers, in
 4 order to gain unauthorized access into the Target Devices and protected computers and networks.

5 144. Through the acts and/or omissions as alleged above, the Corporate Defendants either
 6 individually or jointly committed and violated 18 U.S.C. § 1030 (a)(2) because they intentionally
 7 initiated Hell Programs and accessed, and caused to be accessed (a) Plaintiff's and Individual
 8 Defendants computers, and protected computers, and (b) Plaintiff's and Individual Defendants
 9 Target Devices allowing unauthorized access with the intent to obtain iHug Trade Secrets and other
 10 data which caused unauthorized login access to Plaintiff's computers and protected computers.

11 145. In one instance of the Corporate Defendants unauthorized access into Target
 12 Devices, during a Twitter War between Cyber Security Experts and Researchers, a Former Apple
 13 Senior Engineering Manager and an Uber employee, it was corroborated that Apple granted Uber
 14 access to private entitlements. More specifically, the premise of the Twitter War pertained to Apple
 15 granting Uber special permissions to sensitive and frightening access to user's screens, and into
 16 Target Devices core registries, including keylogging capabilities. Keylogging allows the Corporate
 17 Defendants to extract and/or observe and/or record each keystroke on a user's Target Device screen,
 18 including the Individual Defendants Target Devices.

19 146. The former Apple Senior Engineering Manager retweeted, attached a screen shot
 20 and stated: "*Yup, can confirm*", referring to Apple granting Uber special access.

21 147. An Uber employee also Tweeted and confirmed that Apple granted Uber special
 22 access and stated: "*API was used to render Uber maps on iphone & send to Apple Watch before*
 23 *Watch apps could handle it. It's not in use & being removed. Thx!*"

24 148. A Security Researcher saw the Uber employees Tweet, and Tweeted, "*If it*
 25 *wasn't being used, why was it pushed to production. Made it all the way from ur branch to the*
 26 *main trunk*".

27 149. The same Uber employee provided a statement to the media as follows, "*Apple gave*
 28

1 *us this permission because of early versions of Apple Watch were unable to adequately handle the*
2 *level of map rendering in the Uber app.”*

3 150. After a Cyber Security Researcher indexed tens of thousands of apps binary using
4 his own company’s internal data set derived from the App Store, he couldn’t find a single app that
5 used the Apple-code that Uber was permitted to use by Apple, except Apple’s native apps. The
6 same Cyber Security Expert further stated in a tweet, “*Granting such a sensitive entitlement to a*
7 *third-party is unprecedented as I can tell, no other app developers have been able to convince Apple*
8 *to grant them entitlements they’ve needed to let their apps utilize certain privileged system*
9 *functionality*”. He went on to state, “*even after [Uber] previously abused" the App Store rules, Uber*
10 *still "convinced Apple to let them have exclusive access to this privileged entitlement."*”

11 151. In a second instance, after a purported white-hat hacker analyzed and reviewed
12 Uber’s access, the researcher stated in an article, “*Essentially it gives you full control over the*
13 *framebuffer, which contains the colors of each pixel of your screen. So, they can potentially draw*
14 *or record the screen, it can potentially steal passwords etc.”*. He went on to state, “*the specific*
15 *entitlement, known as ‘com.apple.private.allow-explicit-graphicspriority’, allows a developer to*
16 *read or write to the iPhone's framebuffer, a part of the phone's memory that contains pixel and*
17 *display data. ‘Writing is always possible from an app using normal rendering services, which draw*
18 *to framebuffer on your behalf,’ he said. "Reading allows you to look at the device's screen."*

19 152. In another instance, another Cyber Security Expert, alleged, it gives “*complete*
20 *access to the targets daily activities, including precise location, complete conversations on even*
21 *the most encrypted channels, and all secure passwords that the target is using”*.”

22 153. During this discovery of unlawful activity, Apple still refused to comment. As set
23 forth above herein, Uber had willfully continued using Hell Programs that Apple knew or should
24 have known was in use. This code is forbidden to be used by any developer except Apple itself. In
25 sum, the former Apple Senior Engineering Manager, Cyber Security Expert and Researchers, and
26 Uber employees all confirmed Apple had in fact granted Uber permissions to access Target Devices,
27 while Apple’s spokesperson refused to comment.
28

1 154. Plaintiff further alleges in on and around early 2020, in an apparent corporate
2 cover-up, two of his Target Devices began simultaneously downloading files and text messages
3 from Apple's servers without prompt or authorization. Plaintiff recorded one of the instances,
4 including a message from Apple stating, "iCloud messages downloading". There was no option,
5 button or other means to stop the data manipulation. Plaintiff had no choice but to allow Apple to
6 complete the forced download to his Target Devices. As set forth above, Uber's former Security
7 Team corroborates these unlawful actions, specifically Uber, "*unlawfully collected information*
8 *from the mobile phones of Uber opponents...*" and, Uber continues to unlawfully use "*secret*
9 *capabilities in Uber's smartphone applications, and offensive intrusions into the privacy of users*".

10 155. The Corporate Defendants and Individual Defendants willful, malicious and
11 unlawful actions caused Plaintiff to incur losses and damages, including his time, and among other
12 things, the expenditure of resources to investigate and remediate the Corporate Defendants and
13 Individual Defendants conduct and damage to Plaintiff, and damage to the relationships and
14 goodwill between Plaintiff and iHug users, and other potential iHug users.

15 156. The Corporate Defendants fraud includes, and not limited to, sending illegal,
16 unauthorized and organized pattern of repeating code execution and computer commands through
17 Hell Programs, Uber's malicious servers, Apple's App Store, Apple's native access methods and
18 infrastructure, Uber's smartphone applications, other apps, and through Target Devices without
19 warning, prompt or authorization into Plaintiff's Target Devices, protected computers, and network
20 computers in order to gain access and ascertain iHug Trade Secrets and other competitive data
21 without consent, authorization and without Plaintiff's knowledge.

22 157. The Corporate Defendants and Individual Defendants violated 18 U.S.C. § 1030(b)
23 by conspiring and attempting to commit the violations alleged in the proceeding paragraphs.

24 158. Their actions caused Plaintiff to incur a loss as defined in 18 U.S.C. § 1030(3)(11),
25 including the expenditure of resources to investigate and remediate the Corporate Defendants and
26 Individual Defendants fraud. Plaintiff is entitled to be compensated for losses and damages, and
27 any other amount to be proven at trial.
28

FIFTH CAUSE OF ACTION

Violation of California Business & Professional Code § 17200

Against All Defendants

159. Plaintiff incorporates all of the above paragraphs as though fully set forth herein.

160. At a market cap of nearly \$2 trillion, Apple's size and reach far exceeds that of any technology monopolist in history, and wields such power to stifle competition as alleged in this Complaint. The Corporate Defendants and Individual Defendants conduct, as described above, violates California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, et seq., which prohibits any unlawful, unfair, or fraudulent business act or practice.

161. Plaintiff has standing to bring this claim because Plaintiff has suffered injury in fact and lost the value of iHug Trade Secrets as a result of the Corporate Defendants unfair competition. Specifically, the Corporate Defendants use of Hell Programs has unreasonably restricted Plaintiff's ability to fairly compete using iHug Trade Secrets.

162. The Corporate Defendants and Individual Defendants engaged in unlawful, unfair, and fraudulent business acts and practices. Such acts and practices are not limited to, misappropriating Plaintiff's confidential and proprietary information, iHug Trade Secrets and other data by initializing a repeating pattern of unauthorized computer access through use of Hell Programs.

163. The Corporate Defendants business acts and practices were unlawful as described above. These acts and practices that were fraudulent and oppressive in that a reasonable person would likely be deceived by their material misrepresentations and omissions and use of Hell Programs

164. The Corporate Defendants have acquired and used Plaintiff's confidential and proprietary trade secret information through material misrepresentations and omissions.

165. Upon information and belief, Plaintiff alleges thereon that Uber freely exploits competitor's Target Devices through use of Hell Programs to observe the formulation of competitor's trade secrets, extrapolates ideas from these trade secrets and launches new services

MACKINTOSH V. APPLE ET. AL.

1 and products derived from these trade secrets, stifling innovation in America, specifically, in
2 California. As a result, Plaintiff has been harmed as a result of the Corporate Defendants and
3 Individual Defendants unlawful, unfair, and fraudulent business acts and practices.

4 166. The Corporate Defendants and Individual Defendants conduct is also “unfair” within
5 the meaning of the Unfair Competition Law.

6 167. During Macworld 1997 presentation available at <https://youtu.be/IOs6hnTI4lw>, the
7 late Steve Jobs passionately said in closing, “*Lastly, I want to talk a little bit about Apple, and the*
8 *brand, and what it means to a lot of us... You know, you always had to be a little different to buy*
9 *an Apple computer... you had to think differently because there wasn't any software at the*
10 *beginning... it was a totally different computer... worked in a totally different way... used a totally*
11 *different part of your brain... and it opened up a computer world to a lot of people who thought*
12 *differently... and I think the people who do buy them, do think differently... they are the creative*
13 *spirits in this world... they are people who are not out to get a job done, they are out to change the*
14 *world... and they are out to change the world using whatever tools they can get... and we make*
15 *tools for those kinds of people.*” Through this core belief, tens of millions of artists, engineers,
16 developers, entrepreneurs, and other creatives grew a deep love and trust for Apple, who use Apple
17 tools **[as described in paragraph 30 in this Complaint]** so they can change the world.

18 168. Plaintiff deeply trusted Apple, who has always thought differently through his
19 inherent creativity and out-of-the-box thinking, who was out to change the world through an AiOS
20 platform using Apple tools. Fast forward to 2020, Plaintiff alleges Apple has violated that deep love
21 and trust, by allegedly aiding and abetting Uber and collectively engaging in unfair competition by
22 using the very same Apple tools against Plaintiff, and other competitors through Hell Programs.

23 169. Plaintiff is entitled to (a) recover restitution, including without limitation, all benefits
24 that the Corporate Defendants and Individual Defendants received as a result of their unlawful,
25 unfair, and fraudulent business acts and practices and (b) further injunctive relief under the Unfair
26 Competition Law restraining the Corporate Defendants and Individual Defendants from engaging
27 in further acts of unfair competition and other acts the Court deems unlawful.

28

SIXTH CAUSE OF ACTION

Conspiracy to violate 18 U.S.C. §§ 1961(5), 1962(d) and § 502

Against All Defendants

170. Plaintiff repeats and re-alleges each and every allegation of the foregoing paragraphs as if fully set forth herein, and specifically repeats and re-alleges the allegations under the Seventh Cause of Action concerning Racketeer Influenced and Corrupt Organizations “RICO” liability. During the ten (10) calendar years preceding 2020, the Corporate Defendants and Individual Defendants cooperated jointly and severally in the commission of at least two (2) or more predicate racketeering acts under the RICO statutes, and engaged in acts that are itemized at 18 U.S.C. §§ 1961(1)(A) and (B), in violation of 18 U.S.C. § 1962(d) as alleged below.

171. Plaintiff further alleges that the Corporate Defendants and Individual Defendants did commit two (2) or more of the offenses itemized above in a manner which they calculated and premeditated intentionally to threaten continuity, i.e. a continuing threat of their respective racketeering activities, also in violation of 18 U.S.C. § 1962(d) (prohibited activities).

172. Specifically, the Corporate Defendants violated the California Comprehensive Computer Data Access and Fraud Act § 502 and Computer Fraud and Abuse Act § 1030 through use of Hell Programs, allowing unauthorized access into Target Devices, and v-machines after the Individual Defendants had compiled iHug Trade Secrets. Plaintiff further alleges, the Corporate Defendants and Individual Defendants conspired and executed on the schemes to access trade secrets as alleged in this Complaint allowing several § 502 and § 1030 violations in an organized, repeating pattern of activity to unlawfully and improperly obtain iHug Trade Secrets.

173. The Corporate Defendants unlawful theft of iHug Trade Secrets and public disclosure and/or storage of the data on malicious servers has destroyed the value of iHug Trade Secrets. Pursuant to sections § 502 and § 1030, Hell Programs inherently cause unauthorized computer access that grants the Corporate Defendants access into Target Devices as alleged above. These modes within each Hell Program cannot be prevented and/or defended against, continue to pose a threat.

MACKINTOSH V. APPLE ET. AL.

AND AS FOR A SEVENTH CAUSE OF ACTION

Racketeer Influenced and Corrupt Organizations 18 U.S.C. § 1961-68

Against All Defendants and DOES

174. Plaintiff incorporates by reference all the preceding paragraphs of this Complaint as if fully set forth herein:

175. Defendants violated the RICO statute and Plaintiff was injured as a result.

176. Each Defendant is a "person" capable of holding legal or beneficial interest in property within the meaning of 18 U.S.C. § 1961 (3).

177. Each Defendant violated 18 U.S.C. 3 1962(c) by the acts described in the prior paragraphs, and as further described below.

Enterprise

178. Defendants, Apple together with (1) Uber and DOES has created Hell Programs (2) specifically Apple aided and abetted Uber with Apple-code and/or knew or should have known Uber used and/or misused Apple-code (3) through Apple-code and Target Devices, v-machines, apps, chats, and use of Apple and/or Uber's Headquarters, hubs and other private locations; with (4) one or more former or current officers and/or directors of Uber (5) one or more former or current officers and/or directors of Apple (6) employees, officers and directors of Uber (7) employees, officers and directors of Apple together with (8) Josef, Wang and DOES forms an association-in-fact for the common and continuing purpose described herein and constitute an enterprise within the meaning of 18 U.S.C. 3 1961 (9) engaged in the conduct of their affairs through a continuing pattern of racketeering activity. There may also be other members of the enterprise who are unknown at this time.

179. Alternatively, Uber is a separate enterprise within the meaning of 18 U.S.C. 1961(4); Apple is a separate enterprise within the meaning of 18 U.S.C. 1961(4); Wang, Josef and DOES collectively or separately, are a separate enterprise within the meaning of 18 U.S.C. 1961(4). Each enterprise has knowing, willfully and maliciously engaged in, and their activities have affected, interstate and foreign commerce.

MACKINTOSH V. APPLE ET. AL.

Isolated Events and Acts

180. The acts of RICO were not isolated, but rather the Corporate Defendants and Individuals Defendants acts were related in that they had the same or similar purpose and result, participants, victims and method of commission.

181. Further, the surreptitious acts by the Corporate Defendants and Individuals Defendants, have been continuous and repeating during a period of time continuing to present, and there is a continued threat of repetition of such conduct through the existence of Apple-code and Apple Products and use of the Individual Defendants, who are influenced, bribed and/or paid to engage in fraud and theft by loading trade secrets onto Target Devices and v-machines, while the Corporate Defendants initiate Hell Programs to access the data without authorization.

Pattern of Criminal Racketeering Activity

182. The Individual Defendants, each of whom are persons associated with, employed by or formally employed by the Corporate Defendants did knowingly, willfully and unlawfully conduct or participate, directly or indirectly, in its affairs through patterns of racketeering within 18 U.S.C. § 1961(1), §1961(5), §1962(c).

Racketeering Acts

183. Predicate acts of racketeering activity are acts which are indictable under provisions of the U.S. Code enumerated in 18 U.S.C. § 1961(1)(B), as more specifically alleged below.

184. Each Defendant committed at least two such acts or else aided and abetted such acts and activity.

185. The activity was made possible by the Corporate Defendants regular and repeated use of the enterprises personnel, facilities, services, servers, and more specifically the use of Apple-code, Hell Programs and all inherent known and unknown modes that inherently cause unauthorized computer access into Target Devices as described throughout paragraphs 1 – 77 and 120 – 174.

186. Each Defendant had the specific intent to engage in the substantive RICO violations alleged herein and throughout paragraphs 1 – 77.

Predicate Act Violation 1

Obstruction of Justice pursuant to 18 U.S.C. § 1961 (1)(B) section 1503

Against All Defendants and DOES

187. For the purpose of executing their fraudulent scheme, each Defendant engaged in destruction, tampering with, and spoliation of evidence with the explicit purpose and with the intent to obstruct justice as follows:

188. Upon a deeper investigation, it was revealed that Wang is a Silicon Valley Hacker. Wang also worked at Apple within a secret project named “M68”, a code name for the development of iPhone before it was unveiled. Wang is presumably very familiar with Apple-code, Apple’s Servers, Target Devices and hacking. After Wang received a settlement demand from Plaintiff alleging his involvement with Uber, Wang permanently deleted his chats with Uber, the Uber Manager, and DOES closing off loose-ends, and setup a bitcoin account to receive ‘illegal hush money payments.’ After the transaction, Wang proceeded to hide his online identity, and closed his post office box where he had received Plaintiff’s settlement demand, and other correspondence including Plaintiff’s payments. Wang subsequently refused and failed to respond to Plaintiff.

189. Upon information and belief, Mackintosh alleges Uber knowingly and with the intent to engage in corporate cover-up, paid illegal hush money payments to two or more individuals, while Wang, Josef and DOES intentionally wiped Target Devices containing encrypted messages, encrypted files, and photographs of Plaintiff’s Trade Secrets and competitive data.

190. Josef also engaged in destruction of digital and forensic evidence, specifically, he unlawfully acquired and destroyed one or more Target Devices belonging to Plaintiff. The Target Devices contained key evidence pertaining to the Corporate Defendants, Josef, Wang and DOES web traffic and internet activity. In a similar fashion as to Wang, Uber also proceeded to engage in wiping at least four or more chats within Uber’s Engineering, MA, and Threat Operation divisions.

191. After Uber received Plaintiff’s settlement demand, Uber terminated thousands of employees within MA, SSG, and other divisions who allegedly have knowledge of activity alleged in this action. On information and belief, Uber also permanently closed offices where Wang, Josef

MACKINTOSH V. APPLE ET. AL.

1 and DOES had met.

2 192. Upon information and belief, Defendants have and continue to surreptitiously
3 initiate Hell Programs on Plaintiff's potential legal counsel's Target Devices to access Plaintiff's
4 draft Complaints, evidence, witness lists, and even legal strategies and defenses to prejudice
5 Plaintiff during litigation and at trial. For instance, after Plaintiff used an emailing program to send
6 his draft Complaint to a four-person law firm located in Sacramento California for potential
7 representation, the email was opened approximately 30 times within the same second and minutes
8 and sporadically thereafter.

9 193. The Corporate Defendants have in fact suppressed Plaintiff from retaining counsel,
10 particularly, after Plaintiff continued providing his draft Complaint to various law firms who were
11 interested in taking the case, upon information and belief, the Corporate Defendants reviewed the
12 draft complaints and progressively engaged in multiple corporate cover-ups, deleted evidence and
13 committed acts of threatening key witnesses as Plaintiff's draft Complaints became clearer and
14 concrete as to the RICO violations among other violations. Plaintiff has had to purchase a flip phone
15 and remains offline to prevent the Defendants from viewing his legal data.

16 194. Plaintiff also discovered that a Google Android device belonging to another key
17 witness had over 50 text messages deleted between approximately September 2018 to early- 2019.
18 Similarly, Plaintiff discovered text messages were also deleted from an old thread on his Target
19 Device without his knowledge, consent, authorization and without prompt.

20 195. Upon later examination, another key piece of photographic evidence on one of
21 Plaintiff's Target Devices was tampered with, specifically, the meta-data. Meta-data changes can
22 only occur from its origination source at Apple. No such features exist within Target Devices that
23 would allow a user to tamper with meta-data.

24 196. Upon information and belief, and on that basis, Mackintosh further alleges thereon
25 that Hell Programs not only allow the theft of trade secrets, it allows the unlawful impersonations
26 of competitor to potentially create forensic evidence and/or tampering of meta-data that could
27 potentially be used to launch potential criminal initiatives against competitors as alleged by Uber's
28

MACKINTOSH V. APPLE ET. AL.

1 former and current security officers, See Ex. A “*Jacobs is aware that the MA team fraudulently*
2 *impersonates riders and drivers on competitor platforms, hacks into competitor networks, and*
3 *conducts unlawful wiretapping*”, and Ex. E., “*the conduct includes potentially criminal initiatives*
4 *against competitors, secret capabilities embedded in Uber’s smartphone applications, and*
5 *offensive intrusions into the privacy of users. The allegations of misconduct were directly supported*
6 *by documents attached to the draft complaint. The defendants believe that some of the misconduct*
7 *may continue to this day.*”

8 197. Upon information and belief, and on that basis, Mackintosh alleges that prior to,
9 during and after the Corporate Defendants unlawful activity as alleged in this Complaint, the
10 Corporate Defendants willfully, knowingly, and continuously exploited various Target Devices that
11 targeted Plaintiff’s key witnesses to this action and other potential future actions. In particular, a
12 business acquaintance to Plaintiff, changed his initial story regarding Josef, involving Josef’s
13 actions. In another instance, another business acquaintance to Plaintiff stated that his text messages
14 were deleted. In yet another instance, upon information and belief, after Plaintiff noticed Uber with
15 a settlement demand, within weeks of Plaintiff speaking with his mother on his Target Device, his
16 mother suddenly and unexpectedly passed. Plaintiff wishes that his mother rest in peace,
17 nonetheless, she was a key witness to this action and other potential actions.

18 198. The continued tampering with key witnesses, the destruction of evidence and other
19 unlawful actions alleged throughout this Complaint by The Corporate Defendants and Individual
20 Defendants, have in fact unlawfully prejudiced Plaintiff, violated Plaintiff’s civil rights and
21 constitutional rights among other inalienable rights, with the intent to obstruct Plaintiff’s justice.

22 199. Even more concerning, instead of Apple removing and banning Uber for violations
23 alleged in this Complaint, Uber remains on the App Store without consequence, and has allowed to
24 continue operating, contrary to Apple’s alleged anti-competitive and unfair business practices to
25 ban Epic Games, *See Case Epic Games, Inc.–v–Apple Inc., 4:20-cv-05640-YGR* from the App
26 Store for wanting to provide their own non-Apple payment methods to users.

27 200. Contrary to Apple’s testimony under oath during a United States Congressional
28

1 Anti-Trust hearing in 2020, upon information and belief, Apple gave Uber special treatment and
 2 *de facto* permissions and access to Apple-code that granted Uber and DOES unauthorized access
 3 into Target Devices without warning, without authorization, and without a competitor's knowledge.
 4 See Bloomberg Article, "Apple believes regulatory scrutiny is reasonable, that the company will
 5 'make no concessions on the facts,' and disputes the characterization that Apple is
 6 anti-competitive.' Available at: [https://www.bloomberg.com/news/articles/2020-07-29/apple-s-](https://www.bloomberg.com/news/articles/2020-07-29/apple-s-cook-says-app-store-opened-gate-wider-for-developers?sref=9hGJlFio)
 7 [cook-says-app-store-opened-gate-wider-for-developers?sref=9hGJlFio](https://www.bloomberg.com/news/articles/2020-07-29/apple-s-cook-says-app-store-opened-gate-wider-for-developers?sref=9hGJlFio) or See Ex. K.

8 201. As set forth above, The Corporate Defendants behavior is not only unethical, it's
 9 unconstitutional. Over a period of many years, The Corporate Defendants have unlawfully amassed
 10 and collected Plaintiff's competitive data without authorization using exploited Target Devices and
 11 Hell Programs, causing the accumulation of data on malicious servers, paired with Hell-type
 12 programs and exploitation of Target Devices, allowing the exploitation of Plaintiff and other users.

13 202. Upon information and belief, not only can the Corporate Defendants alter, tamper
 14 with, spoil, delete, fabricate or otherwise manipulate competitive data they collected on Plaintiff,
 15 they can impersonate and target associated and/or unassociated users to Plaintiff, causing harm and
 16 damages with the intent to obstruct Plaintiff's justice, and obstruct an ongoing investigation into
 17 the Corporate Defendants, while tampering with key witnesses using data within their Target
 18 Devices, with the intent to blackmail them into actions targeted at obstructing Plaintiff's justice.

19 203. Even more detrimental to Plaintiff's justice, upon information and belief, on their
 20 own whim, at their own discretion, and on their own volition, the Corporate Defendants can access
 21 mass amounts of data it collects on competitors without probable cause, and/or potentially creates
 22 probable cause by exploiting competitors through their Target Devices, and accesses the data
 23 without first obtaining a subpoena or Court order.

24 204. These acts overrule the powers The People have bestowed upon the United States
 25 Congress and our entire judicial system, who are appointed to protect our inalienable and God given
 26 rights under the Bill of Rights, the United States Constitution and other rights woven within the
 27 fabric of the United States of America.

28

Predicate Act Violation 2

Obstruction of Criminal Investigations pursuant to 18 U.S.C. § 1961 (1)(B) section 1510

Against All Defendants and DOES

205. The Corporate Defendants and Individual Defendants destroyed evidence and key pieces of evidence at all times relevant to this action with the express intent to obstruct an ongoing criminal DOJ investigation as alleged above in paragraphs 187 – 204.

206. The cover-up efforts were intended to conceal the mass theft of iHug Trade Secrets.

207. On information and belief, and on that basis, The Corporate Defendants accessed Target Devices without authorization belonging to witnesses, key witnesses, and iHug personnel, their friends, family and business acquaintances to tamper with, delete and fabricate evidence to prejudice Plaintiff during litigation as alleged above in paragraphs 187 – 204.

Predicate Act Violation 3

Economic Espionage and Theft of Trade Secrets pursuant to 18 U.S.C. § 1961 (1)(B) section

1832 Against Apple, Uber and DOES

208. As set forth above, an amendment was made under RICO 18 U.S.C. §§ 1961-68. The amendment added economic espionage and, particularly pertinent here, theft of trade secrets to the list of predicate offenses that may be considered "racketeering activity."

209. It has become clear and concrete that Uber has conspired with Apple, and DOES to participate in a pattern of racketeering activity as alleged in this Complaint.

210. Plaintiff hereby restates and realleges the allegations set forth in paragraphs 1 – 77, 119 – 173, and 187 – 207.

211. The Corporate Defendants injured Plaintiff and violated the Economic Espionage and Theft of Trade Secret Act pursuant to 18 U.S.C. § 1961 (1)(B) section 1832) by (a) conspiring to use, and used; (b) associated Individuals Defendants, specifically Wang, Josef and DOES; (c) to conduct the operation of access and compiling intellectual property, competitive intelligence and iHug Trade Secrets onto Target Devices and v-machines; (d) while the Corporate Defendants initiate Hell Programs causing unauthorized computer access into the Target Devices and

1 v-machines (e) with the intent to convert the misappropriated iHug Trade Secrets and utilized the
 2 iHug Trade Secrets within the Corporate Defendants business divisions in some way or fashion.

3 212. The Corporate Defendants continue to, and threaten to conspire with associated
 4 individuals to access their Target Devices and relay competitive intellectual property and trade
 5 secrets from the associated individuals Target Devices to Uber's malicious servers and other
 6 cloud-based servers and/or extrapolates ideas from the trade secrets to illegally profit from the
 7 surreptitious theft and continued concealment of the methods of theft by denying the existence or
 8 non-use of Apple-code and Hell Programs.

9 213. The Individual Defendants will continue their patterns of racketeering in a common
 10 and continuing purpose of the Corporate Defendants enterprises.

11 **Predicate Act Violation 4**

12 **Criminal Infringement of a Copyright pursuant to 18 U.S.C. § 1961 (1)(B) section 2319 and**
 13 **18 U.S.C. § 371 Against Uber and Apple**

14 214. Plaintiff's codebase and AiOS patent draft contains a substantial amount of original
 15 material (including without limitation codebase, sketches, formulas, equations within the formulas,
 16 flow charts, figures, marketing and advertising material, specifications, documentation and other
 17 materials) that is protected and copyrighted subject matter pursuant to RICO statute, section 2319
 18 among other U.S. copyright laws.

19 215. Without consent, authorization, approval, or license, the Corporate Defendants
 20 knowingly, willingly, and unlawfully copied, prepared, published, and distributed Plaintiff's
 21 copyrighted work, portions thereof, or derivative works and continues to do so.

22 216. The Uber Health platform infringes Plaintiff's copyrighted codebase and AiOS
 23 patent draft and Uber is not licensed to do so.

24 217. On information and belief, and on that basis, Plaintiff alleges consumer, business
 25 and government users of Uber Health and other divisions at Uber, including Uber Eats new platform
 26 features, must obtain and use copyright portions of the codebase and AiOS patent draft or works
 27 derived therefrom to use and provide features, products and services in healthcare. Such use is not
 28

1 licensed.

2 218. The Corporate Defendants have thus induced, caused, and materially contributed to
3 the illegal infringing acts of others by encouraging, inducing, allowing and assisting others to use,
4 copy, and distribute Plaintiff's codebase and AiOS patent draft copyrightable works, and works
5 derived therefrom.

6 219. On information and belief, the Corporate Defendant's direct and induced illegal
7 infringements are and have been knowing and willful. By this unlawful acquisition and copying,
8 use, and distribution, the Corporate Defendants have violated Plaintiff's codebase and AiOS patent
9 draft rights to inflate the ultimate valuation of Uber, and their investments.

10 220. The Corporate Defendants have realized unjust profits, gains and advantages as a
11 proximate result of its infringement.

12 221. The Corporate Defendants continue to realize unjust profits, gains and advantages
13 as a proximate result of its illegal infringement as long as such illegal infringement is permitted to
14 continue. Plaintiff is entitled to injunctive relief restraining the Corporate Defendants and DOES
15 from engaging in any further such acts in violation of the RICO act 18 U.S.C. § 1961-68 and
16 sections therein.

17 222. Unless Uber and Apple are enjoined and prohibited from infringing Plaintiff's
18 codebase and AiOS patent draft copyrights, inducing others to infringe codebase and AiOS patent
19 draft copyrights, and unless all infringing products and advertising materials are seized, Corporate
20 Defendants will continue to intentionally infringe and induce infringement of Plaintiff's AiOS
21 copyrights.

22 223. As a direct and proximate result of the Corporate Defendants direct and indirect
23 willful and illegal copyright infringement and unjust enrichment, Plaintiff has suffered, and will
24 continue to suffer, monetary loss to its business, reputation, and goodwill.

25 224. Plaintiff is entitled to recover from the Corporate Defendants, in amounts to be
26 determined at trial, the damages sustained and will sustain, and any gains, profits, and advantages
27 obtained by the Corporate Defendants as a result of the Corporate Defendants acts of illegal
28

1 infringement use, and publication of the copied materials.

2 225. As set forth above, Uber's healthcare operation bears a near-identical operation
3 that's outlined in Plaintiff's patent draft, among other misappropriated iHug Trade Secrets that
4 formed the AiOS. Further, Apple Watch and Apple Health have a near-identical conceptualization
5 and various operations, that are outlined in iHug Trade Secrets in which he was oppressed and
6 obstructed from pursuing and developing through the unlawful acts alleged in this Complaint.

7 **Predicate Act Violation 5**

8 **Offenses related to Bribery pursuant to 18 U.S.C. § 1961 (1)(A)**

9 **Against Uber, Josef, Wang and DOES**

10 226. Upon information and belief, and on that basis, Uber devised and executed a scheme
11 artifice to defraud and deceive competition, specifically Plaintiff, by forming a fraudulent method
12 of creating fake rider and driver accounts for Josef and DOES who receive inflated payments
13 through such fictitious accounts. Mackintosh further alleges, after Josef and DOES complete a
14 confidential assignment, Uber proceeds to permanently delete the fake driver accounts after deposit
15 and/or other methods of transferring payments. Bitcoin cryptocurrency was also a method of
16 payment Uber has used in the past to engage in corporate cover-up, with which Wang and DOES
17 utilized after each alleged theft. In particular, at strategic times, after Wang, an Uber Manager, and
18 DOES deleted their chats and created new chats, they proceeded to setup bitcoin in a repeating
19 pattern of organized code execution to receive illegal hush money payments, effectively bribing
20 them from talking or responding to those who claim Uber has harmed them.

21 227. Upon information and belief, Wang, the Uber Manager, Josef and DOES were paid
22 something of value after they built Uber's features and assisted in the evolvement of Uber's
23 platform and operation after loading their v-machines and Target Devices with iHug Trade Secrets.
24 These activities aided and abetted and permitted the Corporate Defendants, to subsequently form
25 entirely new divisions, and evolved existing business operations, including secret divisions within
26 Apple, and other divisions that bear an identical resemblance to iHug Trade Secrets, codebase, and
27 other data while Wang, Josef and DOES were paid and/or paid in some form, way or fashion.

MACKINTOSH V. APPLE ET. AL.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter judgment against Defendants and grant Plaintiff the following relief:

1. That the Court enter judgement as follows for:

- a. Violating the Defense of Trade Secrets Act;
- b. Violating the California Uniform Trade Secret Act, in violation of Cal. Civ. Code §§ 3426, et seq.;
- c. Violating the Computer Fraud and Abuse Act;
- d. Violating the Racketeer Influenced and Corrupt Organizations, in violation of 18 U.S.C. § 1961 and § 1962, and all predicate acts alleged above herein;
- e. Violating the California Comprehensive Computer Data Access and Fraud Act, in violation of Penal Code § 502;
- f. Violating the California Business & Professional Code § 17200;
- g. Violating a United States Permanent Injunction against Uber, *See* Ex. L.;
- h. Conspiracy to violate 18 U.S.C. §§ 1961(5), 1962(d), § (502) and § (1030);

2. That the Court enter a preliminary and permanent injunction against the Corporate Defendants and its officers, agents, servants, employees, successors, assignees, subsidiaries, parents and/or those in active concert with or conspiracy with any of them or who are affiliated with Defendants from:

- a. Accessing or attempting to access iHug's services, platforms, and computer systems;
- b. Accessing or attempting to access Plaintiff, and other Target Devices to obstruct or otherwise alter the nature or result of this action;
- c. Creating or maintaining any iHug account;
- d. Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of iHug computers, computer systems, and computer networks or the iHug service;

- 1 e. Engaging in any activity, or facilitating others to do the same, that violates iHug's
- 2 terms, and/or any applicable laws;
- 3 f. Any association and participation with Uber and Apple prohibiting the use of iHug
- 4 Trade Secrets and anything derived from it within any division and or person(s)
- 5 directly or indirectly related or partnered with Apple and Uber, and order Uber to
- 6 transfer Uber Health, LLC and all interest to Plaintiff;
- 7 g. Engaging in the unlawful behavior of initiating Hell Programs on Plaintiff and his
- 8 potential legal counsel so that Plaintiff can successfully retain counsel.
- 9 3. Plaintiff be awarded trebling damages, and reasonable royalty.
- 10 4. Exemplary damages in an amount not exceeding twice the award of
- 11 compensatory damages pursuant to Cal. Civ. Code § 3246.3 (c) or whichever is greater.
- 12 5. Exemplary damages pursuant to Cal. Civ. Code § 3294 in an amount to
- 13 proven at trial.
- 14 6. For attorneys' fees and costs upon Plaintiff's retention of legal counsel.
- 15 7. Issuing an injunction prohibiting Apple and Uber's anti-competitive conduct and
- 16 mandating that Apple and Uber take all necessary steps to cease unlawful conduct and to restore
- 17 competition, specifically use of Hell Programs or otherwise Apple's native access methods into
- 18 Target Devices.
- 19 8. Plaintiff seeks an accounting of the Corporate Defendant's ill-gotten profits in an
- 20 amount to be determined at trial, and the Corporate Defendants be ordered to disgorge all benefits,
- 21 profits, and/or gains it has realized from use of the Trade Secrets of technology derived therefrom,
- 22 and an order requiring Uber to transfer Uber Health, LLC and all right, title, and interest to
- 23 Mackintosh as Uber Health, LLC was founded on iHug Trade Secrets.
- 24 9. For a constructive trust for the benefit of Plaintiff to be imposed upon all
- 25 funds, assets, revenues and profits derived from the unlawful acts and theft of iHug Trade Secrets.
- 26 10. Apple and Uber be ordered to turn over to Plaintiff, all chats, Hell Programs,
- 27 Apple-code, and other internal systems and servers for forensic review.
- 28

1 11. That the Court enter judgement tolling statutes as a result of each Defendant's
2 fraudulent, willful, calculated and malicious concealment of their unlawful activity, and
3 exploitation of Target Devices that resulted in tampering with Plaintiff's key witnesses, and deleted,
4 altered, created and or otherwise tampered with key pieces of evidence to this action and other
5 potential actions as alleged above.

6 12. For prejudgment and post-judgment interest at the maximum legal rate, as
7 provided by the laws of the State of California and any Federal laws, as applicable with a common
8 result, as an element of damages that Plaintiff has suffered as a result of the violations complained
9 of herein.

10 13. As set forth above, under the following alleged facts of this action, Plaintiff
11 requests that the Court appoints attorneys, and/or assigns pro bono attorneys under the federal pro
12 bono project to assist Plaintiff under this rare circumstance, due to the sensitive and landmark case
13 law this action may create.

14 14. That the Court issue an immediate order seizing and/or confiscating what the Court
15 deems to be The Corporate Defendants proceeds from the alleged acts and associated crimes, and/or
16 an order of forfeiture of assets of the Corporate Defendants to restrain the conduct alleged in this
17 Complaint.

18 15. That the Court issue an immediate witness protective order to the extent the Court
19 deems proper.

20 16. That the Court allow Plaintiff leave to amend this complaint to include recovery of
21 attorneys' fees upon retention of legal counsel, in the event the Corporate Defendants are ordered
22 to cease and desist from allegedly initializing Hell Programs on Plaintiff's potential legal counsel's
23 Target Devices.

24 17. Awarding any other equitable relief necessary to prevent and remedy Apple and
25 Uber's anti-competitive conduct.

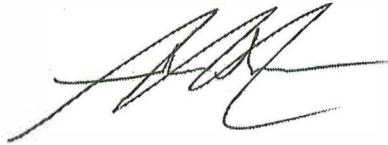
26 18. That Plaintiff ("Mackintosh") be awarded such other and further relief as the Court
27 deems equitable and just.

28

1 **PLAINTIFF RESPECTFULLY DEMANDS A JURY TRIAL**

2
3 Dated: December 23, 2020

Respectfully submitted,

4
5
6 

7 ADAM JOHN MACKINTOSH

8 *Pro Se*

9 legal@ihughealth.com

10 (415) 767-0097

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
MACKINTOSH V. APPLE ET. AL.